AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with the two email accounts listed in Attachment A-1 that is stored at premises controlled by Microsoft Corporation USA	)	Case No. 3:23-mj-174

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Western District of Washington *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B-1

YOU ARE COMMANDED to execute this warrant on or before 5/12/23 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Signatory Magistrate Judge.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 4/28/23 4:35pm

Peter B. Silvain, Jr.
United States Magistrate Judge

City and state: Dayton, OH

Return

Case No.: 3:23-mj-174	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1
Property to Be Searched

Information associated with the email accounts **billdaniel2@msn.com** and **brdljdas@hotmail.com** that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation USA, a company that accepts service of legal process at 1 Microsoft Way, Redmond, Washington, 98052.

ATTACHMENT B-1
Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation USA (the "Provider")

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1 for the time period of January 1, 2019 to the present:

1. All account registration details, billing address, and all other records or information regarding the identification of the account, including full name, physical address, telephone numbers and other identifiers, the date and time when the account was created, the IP and MAC addresses used to register the account, the length of service, the types of service utilized, records of session times and durations, login IP and MAC addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account numbers);
2. All billing information for the account, including billing address, payment instruments, and billing transaction history;
3. All IP logs and session details for the accounts;
4. All privacy settings and other account settings, including privacy settings for individual activities, and all records showing which users have been blocked by the account;
5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;
6. For the accounts listed in Attachment A-1, all Microsoft accounts that are linked to any of the accounts listed in Attachment A-1 by cookies, creation IP address, recovery email address, and/or telephone number;
7. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2251(a) and (e) (conspiracy to produce child pornography); 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography); and 18 U.S.C. §§ 2251(a)(4)(A) and (b)(2), 2252(a)(4)(B) and (b)(2), and 2252A(a)(5)(B) and (b)(2) (possession of child pornography), from January 1, 2019 to the present, including but not limited to the following:

1. Any records related to the possession, receipt, distribution, and production of child pornography.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any Internet history indicative of searching for child pornography.
5. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
6. Any communications with minors.
7. Any communications with or about individuals identified in the Affidavit as "Adult Female-1", "Minor A", and "Minor B".
8. Evidence of utilization of email accounts, messenger applications, social media accounts, online chat programs, and peer-to-peer file sharing programs.
9. Evidence of utilization of the PayPal, CashApp, and Western Union applications.
10. Evidence of utilization of the eBay application.
11. Lists of computer and Internet accounts, including user names and passwords.
12. Any information related to the use of aliases.
13. Any records, documents, and billing records pertaining to accounts held with telephone, electronic, and Internet service providers.
14. Any and all diaries, notebooks, notes, and other records reflecting personal contact and any other activities with minors.
15. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
16. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
17. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
18. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.